访问控制

2020年5月20日 16:56

1. 访问控制：限制访问主体（发起者）对访问客体（需要保护的资源）的访问权限，从而使计算机系统在合法范围内使用。访问控制机制决定用户及代表一定用户利益的程序能做什么，以及做到什么程度
    a. 通过认证来检验主体的合法身份
    b. 通过授权（Authorization）来限制用户对资源的访问级别
2. 基本概念
    a. 主体（Subject）
        i. 访问的发起者，通常包括人、进程和设备
        ii. 根据主体权限不同可以分为四类：特殊用户、一般用户、审计用户、作废的用户
    b. 客体（Object）
        i. 接受访问的被动实体
        ii. 通常包括文件和文件系统、磁盘和磁带卷标、远程终端、信息管理系统的事务处理及其应用、数据库中的数据、应用资源等
    c. 访问（Access）：使信息在主体和客体之间流动的一种交互方式
    d. 访问许可（Access Permissions）：决定了谁能够访问系统，能访问系统的何种资源以及如何使用这些资源
    e. 控制策略：主体对客体的访问规则集，直接定义了主体对客体的作用行为和客体对主体的条件约束
3. 访问控制策略
    a. 自主访问控制（Discretionary Access Control，DAC）：根据主体的身份及允许访问的权限进行决策
        i. 自主是指具有某种访问能力的主体能够自主地将访问权的某个子集**授予其它主体**
        ii. 灵活性高，被大量采用
        iii. 缺点：信息在移动过程中其访问权限关系会被改变。如用户A可将其对目标O的访问权限传递给用户B,从而使不具备对O访问权限的B可访问O
        iv. 实现机制主要有：访问控制矩阵、访问控制列表、访问控制能力列表
    b. 强制访问控制（Mandatory Access Control，MAC）：每个用户及文件都被赋予一定的安全级别，系统通过比较用户和访问的文件的安全级别来决定用户是否可以访问该文件
        i. 用户不能改变自身或任何客体的安全级别，即不允许单个用户确定访问权限，**只有系统管理员可以**确定用户和组的访问权限
        ii. 安全级别一般有五级：绝密（Top Secret）、秘密（Secret）、机密（Confidential）、限制（Restricted）和无密（Unclassified）
    c. 基于角色的访问控制（Role-based Access Control，RBAC）：将访问许可权分

配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权

i. 角色成为访问控制中访问主体和受控对象之间的一座桥梁
ii. 角色**由系统管理员定义**，角色成员的增减也只能由系统管理员来执行，即只有系统管理员有权定义和分配角色
iii. 用户与客体无直接联系，他只有通过角色才享有该角色所对应的权限，从而访问相应的客体。因此用户不能自主地将访问权限授给别的用户

d. 基于任务的访问控制（Task-based Access Control，TBAC）：对象的访问权限控制并不是静止不变的，而是随着执行任务的上下文环境发生变化
   i. TBAC模型由工作流、授权结构体、受托人集、许可集四部分组成
   ii. TBAC模型一般用五元组（S，O，P，L，AS）表示，其中S表示主体，O表示客体，P表示许可，L表示生命期（Lifecycle），AS表示授权步
   iii. TBAC从工作流中的任务角度建模，可以依据任务和任务状态的不同，对权限进行动态管理。因此，TBAC**非常适合分布式计算和多点访问控制的信息处理控制以及在工作流、分布式处理和事务管理系统中的决策制定**
e. 基于对象的访问控制（Object-based Access Control，OBAC）：将访问控制列表与受控对象或受控对象的属性相关联，并将访问控制选项设计成为用户、组或角色及其对应权限的集合
   i. 允许对策略和规则进行**重用、继承和派生**操作。派生对象可以继承父对象的访问控制设置
   ii. 可以减轻由于信息资源的派生、演化和重组等带来的分配、设定角色权限等的工作量

4. 自主访问控制的实现机制
   a. 访问控制矩阵：利用二维矩阵规定任意主体和任意客体间的访问权限，矩阵中每行代表一主体的访问权限属性，每列代表一客体的访问权限属性，每格表示所在行的主体对所在列的客体的访问授权
   b. 访问控制列表：以文件为中心建立访问权限表，表中登记了客体文件的访问用户名及访问权隶属关系
   c. 访问控制能力列表：以用户为中心建立访问权限表，为每个主体附加一个该主体能够访问的客体的明细表
5. 访问控制应用
   a. MAC地址过滤
   b. VLAN隔离
   c. ACL访问控制列表
      i. 维护该访问控制列表不仅耗时，而且较大程度上增加了路由器开销
   d. 防火墙访问控制